Attorney's Docket No. 5577-357/RSW920010221US1   <u>PATENT</u>

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Brabson *et al.*   Confirmation No.: 3354
Serial No.: 10/007,446   Group Art Unit: 2132
Filed: December 5, 2001   Examiner: Kristin D. Sandoval
For: **POLICY-DRIVEN KERNEL BASED SECURITY IMPLEMENTATION**
                              CONTROL

Date: June 22, 2006

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

```
CERTIFICATION OF TRANSMISSION

I hereby certify that this correspondence is being transmitted
electronically to the U.S. Patent and Trademark Office on June 22,
2006.

Traci A. Brown
```

REASONS IN SUPPORT OF APPLICANTS'
PRE-APPEAL BRIEF REQUEST FOR REVIEW

This document is submitted in support of the Pre-Appeal Brief Request for Review that is filed concurrently herewith along with a Notice of Appeal in compliance with 37 C.F.R. 41.31 and with the rules set out in the OG Notice of July 12, 2005 for the New Appeal Brief Conference Pilot Program.

It is not believed that an extension of time and/or additional fee(s)-including fees for net addition of claims-are required, beyond those that may otherwise be provided for in documents accompanying this paper. In the event, however, that an extension of time is necessary to allow consideration of this paper, such an extension is hereby petitioned under 37 C.F.R. §1.136(a). Any additional fees believed to be due in connection with this paper may be charged to our Deposit Account 09-0461.

REMARKS

Applicants hereby request a Pre-Appeal Brief Review (hereinafter "Request") of the claims finally rejected in the Final Office Action mailed March 23, 2006 ("Final Office Action") and the Advisory Action mailed June 8, 2006 ("Advisory Action"). The Request is provided herewith in accordance with the rules set out in the OG Notice of July 12, 2005.

Applicants submit that the rejections are based on a clear error in understanding the applied references, and that the Final Office Action and Advisory Opinion have failed to establish a case of prima facie obviousness with respect to the rejected claims. Accordingly, Applicants request review of the present application by an appeal conference prior to the filing of an appeal brief. In the interest of brevity and without waiving the right to argue additional grounds should this Petition be denied, Applicants will only discuss some particular errors made in the rejections of independent Claims 1, 17 and 18.

In the Final Office Action, Claim 1 was rejected as anticipated by U.S. Patent No. 5,029,206 to Marino, et al. ("Marino"), while Claim 3 was rejected as unpatentable over Marino in view of U.S. Patent No. 6,131,163 to Wiegel ("Wiegel"). In an Amendment After Final filed May 17, 2006, Applicants requested entry of an amendment of Claim 1 to include the recitations of Claim 3. The Advisory Action indicated that the amendment would be entered, but stated that Claim 1, as amended, would be rejected on the same grounds as Claim 3. Accordingly, Applicants will discuss the rejection of Claim 1, as amended.

Claim 1, as amended, recites as follows (emphasis added):

1.   A method of improving security processing in a computing network, comprising:
        providing security processing in an operating system kernel;
        providing an application program which makes use of the operating system kernel during execution;
        providing security policy information that is usable for more than one executing application program;
        executing the application program; and
        selectably encrypting at least one communication of the executing application program using the provided security processing in the operating system kernel, under conditions specified by the security policy information.

Claims 17 and 18 contain similar recitations as Claim 1. Thus, the discussion below with respect to Claim 1 applies equally to Claims 17 and 18.

Briefly, Applicants submit that neither Marino nor Wiegel, alone or in combination, discloses selectably encrypting at least one communication of an executing application program using security processing provided in an operating system kernel, under conditions specified by security policy information that is usable for more than one executing application program, as recited in Claim 1.

In the Amendment After Final, Applicants explained that, in the system of Marino, security processing in the kernel relies on information provided to the security processing modules by the application programs that generate the information to be encrypted. See Amendment After Final, p. 8, last paragraph to p. 9, first paragraph. This is in direct contrast to Claim 1, which recites selectably encrypting a communication of an executing application program using security processing in the operating system kernel, under conditions specified by security policy information that is usable for more than one executing application program. Since the security processing of Marino is performed in response to security parameters passed by individual programs, the security processing of Marino is not performed under conditions specified by security policy information that is usable for more than one executing application program. Moreover, there is no indication in Marino that the parameters passed by an application to the security modules described therein are usable for more than one application program.

The Final Office Action stated that Wiegel teaches a method wherein the security policy information is usable for more than one executing application program. Final Office Action, p. 3. However, Applicants have explained in the Amendment After Final that Wiegel relates to a system for managing port-level system requests. See, e.g., Amendment After Final, p. 9, fifth paragraph. Wiegel describes the use of a "policy tree" that is a representation of an abstract security policy that can instruct the system to <u>accept or reject</u> a data packet based upon criteria relating to the data packet. Wiegel, col. 9, ll. 38-41. Thus, the "policy tree" of Wiegel does not correspond to "security policy information" as recited in Claim 1 that provides conditions for selectably <u>encrypting</u> a communication of an application program. Thus, even if Wiegel and Marino were combined, the resulting system would not provide a system that selectably encrypts a communication of an executing application program using security processing provided in the operating system kernel, under conditions specified by security policy information that is usable for more than one application program, as recited in Claim 1.

In the Amendment After Final, Applicants further argued that there is no motivation to combine Marino and Wiegel in an attempt to produce the claimed invention. See Amendment After Final, p. 9, last paragraph to p. 11, first paragraph. In particular, Applicants noted that Wiegel relates to port-level security processing (i.e. accepting or rejecting packets based on predetermined acceptance criteria).

The Advisory Action stated that a skilled person would be motivated to combine Marino and Wiegel because Marino states that it has, as an object, providing a uniform system interface for cryptographic services, key management services and system management services in a single kernel, and that since Wiegel relates to secure system management services, it would be combined with Marino to protect a system and its services from attacks outside a network at the kernel level using its security policies. Advisory Action, p. 2. However, the combined system hypothesized in the Advisory Action is not the subject matter to which Claim 1 is directed. That is, Claim 1 is directed to securing communications of an application program, not securing a system against attacks outside a network. Thus, the Advisory Action essentially admits that even if Marino and Wiegel were combined, it would simply provide the system of Marino with port-level security processing as described in Wiegel, and would not suggest a system that selectably encrypts a communication of an executing application program using provided security processing in the operating system kernel, under conditions specified by security policy information that is usable by more than one application program, as recited in Claim 1.

The dependent claims are patentable per the patentability of the independent claims from which they depend. Accordingly, Applicants respectfully request that the present application be allowed.

Respectfully submitted,

David C. Hall
Registration No. 38,904

USPTO Customer No. 46589
Myers Bigel Sibley & Sajovec
Post Office Box 37428
Raleigh, North Carolina 27627
Telephone: 919/854-1400
Facsimile: 919/854-1401